



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6

DISTRIBUTION: A, B, C, J, S

CJCSI 6610.01B

30 November 2003

TACTICAL DATA LINK STANDARDIZATION IMPLEMENTATION PLAN

References: See Enclosure C.

1. Purpose. This instruction establishes policy to achieve and maintain interoperability among those Department of Defense (DOD) National Security Systems (NSS) that implement tactical data links (TDLs). Policies outlined in this instruction are focused on achieving interoperability through the standardization of message format, content and, implementation. In accordance with DOD Directive 4630.5 (reference a), this instruction establishes procedures for the development, review and validation of NSS TDL message standards based on compatibility, interoperability, and integration requirements. It also establishes procedures for ensuring compliance through joint interoperability certification and program review. As directed by DOD Instruction 4630.8 (reference b), it establishes procedures for the validation of interface standards and compatibility requirements for TDL message format and content. Applicable TDL interface standards are found in Enclosure A.

2. Cancellation. CJCSI 6610.01A, 5 January 2001, is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Military Departments, and DOD agencies and activities. It is also recommended for other federal departments implementing TDLs. The Joint Multi-Tactical Data Link Configuration Control Board (JMTCCB) Terms of Reference (reference c), Joint Multi-Tactical Data Link Standards Working Group (JMSWG) Terms of Reference (reference d) and the DOD Information Technology Standards Management Plan (reference e) establish TDL configuration management procedures.

4. Policy. DOD NSS implementing TDLs will comply with applicable TDL message standards (Enclosure A) and their associated documentation.

Compliance with TDL message standards is fundamental to achieving and maintaining joint and combined compatibility and interoperability.

a. Documentation. TDL message standards are defined in US military standards (MIL-STD) documents and North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs). Joint Multi-Tactical Data Link Operating Procedures are contained in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6120.01 (reference f).

b. Certification Requirements, Minimum Implementation Exceptions and Interim Authority to Operate (IATO).

(1) In accordance with CJCSI 6212.01 (reference g), all NSS that implement TDLs are considered for joint use. Joint certification is required prior to operating in joint or multi-national arenas. The Military Communications-Electronics Board's (MCEB's) interoperability test panel (ITP) and DOD interoperability senior review panel (ISRP) will review platforms that deploy without joint certification for consideration and possible inclusion on the interoperability watch list (IWL).

(2) Compliance with minimum implementation requirements contained in TDL message standards is an essential element in ensuring interoperability. In some instances, however, a NSS TDL may support a mission so narrowly defined it would be undesirable to comply with all elements of the required minimum implementation. In these cases the JMTCCB may approve exceptions to minimum implementation requirements. In accordance with its responsibility as Joint Force Integrator, the US Joint Forces Command (USJFCOM) representative to the JMTCCB must concur in any minimum implementation exceptions by evaluating user requirements and weighing the interoperability impact. Normally, exceptions will be approved in advance of TDL system joint interoperability certification testing. Exceptions are intended to be permanent and will be included in all system description documentation. Approved exceptions do not constitute a waiver of the requirement for any TDL system to complete Defense Information Systems Agency (DISA) (Joint Interoperability Test Command (JITC)) joint certification testing.

(3) IATO -- (defined in reference g) is approved by the Joint Staff MCEB ITP. IATO is temporary (may not exceed 1 year in duration) and is appropriate only in exceptional cases where TDL systems are required to deploy for operational necessity. This includes TDL systems that have a JITC joint interoperability test schedule, but will not achieve JITC certification prior to deploying. IATO does not waive the requirement to complete DISA (JITC) joint certification testing.

c. Configuration Management. The DISA Interoperability Directorate (IN), Military Command and Control Standards Division is responsible for

configuration management of TDL MIL-STDs, CJCSM 6120.01, and other associated documents. DISA is the US custodian for applicable US and NATO TDL documents.

(1) The JMSWG is the forum for resolving interoperability issues related to TDL message standards format, structure, and development. The JMTCCB is the configuration management authority for TDL MIL-STDs, applicable NATO STANAGs, CJCSM 6120.01, and other associated US and NATO TDL documents. Action officer review of these documents will be accomplished within the JMTCCB. Following JMTCCB review, updates to CJCSM 6120.01 will be provided to combatant commands, Services and Defense agencies (C/S/A) for concurrence or nonconcurrence only. This staffing procedure is established in order to maintain the rigor of the configuration management process. Recommended changes to CJCSM 6120.01 may be submitted to appropriate JMSWG and JMTCCB representatives, the Joint Staff Communications, and Computer Networks Division (J-6T) or DISA at any time.

(2) In accordance with reference e, each C/S/A will participate in the Information Technology (IT) standards process. In accordance with references c and d, USJFCOM will represent combatant commanders at the JMSWG and JMTCCB. Representatives are responsible for providing their respective organization's position on all issues. Representatives will be empowered to commit their organization's assistance in matters requiring coordination.

d. Migration Strategy. In accordance with the Joint Tactical Data Link Management Plan (JTDLMP - reference h), one method for achieving TDL interoperability is through migration of non-interoperable legacy TDL message standards to the joint family of TDL message standards described in that document. Adherence to JTDLMP policy will be a factor in consideration of IATO requests, interoperability certification and joint message standard development.

e. Joint Interoperability of Tactical Command and Control Systems (JINTACCS) Transformation. The C/S/A will continue building on existing initiatives and those pursued by the Single Integrated Air Picture -- System Engineering Task Force (SIAP-SE TF) to transform the JINTACCS program, including improving interoperability planning, interoperability systems management and requirements identification and prioritization. C/S/A will also continue to develop a process for analyzing information exchange requirements and for defining, managing and assessing bit-level information processing and display functions.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A


7. Summary of Changes

- a. Clarify interim authority to operate procedures and guidance.
- b. Add joint interoperability of tactical command and control systems transformation paragraph.
- c. Harmonize instruction with various related administrative changes (newer references, name changes to groups/organizations etc).

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
<http://www.dtic.mil/doctrine>. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This document is effective immediately.

For the Chairman of the Joint Chiefs of Staff


JAMES A. HAWKINS
Major General, USAF
Vice Director, Joint Staff

Enclosures:

- A - Responsibilities
- B - TDL Standards Publications
- C - References
- GL - Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
Office of the Assistant Secretary of Defense for Networks and Information Integration	2
Office of the Under Secretary of Defense for Acquisition, Technology and Logistics	2
Office of the Secretary of Defense Chief Information Officer	1
Office of the Secretary of Defense for Production and Logistics	1
National Defense University	1
Joint Forces Staff College	1
Air Combat Command	1
Air Force Command, Control, Intelligence, Surveillance and Reconnaissance Center	1
Air Force Doctrine Center	1
Commander Forces Command	1
Commander Forces Command, Joint Interoperability Division	1
Defense Information Systems Agency	1
Defense Information Systems Agency Joint Interoperability Test Command	1
Joint Doctrine Center	1
Joint Spectrum Center	1
Industrial College of the Armed Forces	1
Joint Command and Control Warfare Center	1
Joint Warfighting Center	1
Military Communications – Electronics Board	1
National War College	1
US Forces Japan	5
US Forces Korea	5
Navy Center for Tactical Systems Interoperability	1
US Army Communications and Electronics Command	1
US Army Missile Command (AMCOM)	1
USMC Tactical Systems Support Agency	1
Missile Defense Agency	1

(INTENTIONALLY BLANK)

ENCLOSURE A
RESPONSIBILITIES

1. Principal Staff Assistants will:

- a. Ensure TDL systems conform to joint TDL message standards.
- b. Ensure TDL systems identified during the Mission Need Statement and the Operational Requirements Document validation process contain directives to implement joint TDL standards and/or STANAGs as appropriate.

2. The Chairman of the Joint Chiefs of Staff will establish procedures for the development, coordination, and review of joint TDL message standards, NATO STANAGs, and other associated documentation for DOD NSS.

3. Services, combatant commands, and DOD agencies will:

- a. Ensure TDL systems implement applicable joint TDL message standards and/or STANAGs.

- b. Identify and provide required corrections and improvements to TDL message standards and/or STANAGs and interface operating procedures and fully participate in the configuration management of these documents in accordance with references c through e.

- c. Ensure fielding plans conform to the joint TDL migration plan outlined in reference h.

- d. Ensure all system and platform specific TDL implementations comply with information exchange requirements (IERs) and other requirements in approved requirements documents and operational and system views of approved integrated architectures. The user communities will independently verify compliance and report significant deficiencies to USJFCOM, the Joint Staff, Service Chief Information Officer (CIO) or DOD CIO, as appropriate, for corrective action.

- e. The C/S/A will continue building on existing initiatives and those pursued by SIAP-SE TF to transform the JINTACCS program, including improving interoperability planning, interoperability systems management and requirements identification, and prioritization. C/S/A will also continue to develop a process for analyzing information exchange requirements and for defining, managing, and assessing bit-level information processing and display functions. Standards management will take into account the requirements of

DODI 4120.24, Defense Standardization Program (DSP, and DOD 4120.24-M, DSP Policies and Procedures.

4. Combatant commands will:

a. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures. In coordination with USJFCOM, fully participate in the configuration management of these documents in accordance with references c through e.

b. Identify through Integrated Priority List submissions the highest priority TDL issues within their area of responsibility, to include data link management, fielded systems that are either not interoperable or not supported, and warfighting capability shortfalls related to TDLs.

5. Directors of the National Security Agency, National Reconnaissance Office and Defense Intelligence Agency will:

a. Ensure TDL systems implement joint TDL message standards as defined by and in accordance with the procedures found in references a through q as appropriate.

b. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures and fully participate in the configuration management of these documents in accordance with references c through e.

6. DISA is executive agent for the Joint Interoperability of Tactical Command and Control Systems program including Link-11, Link-11B, Link-4A, Link-16, Army Tactical Data Link (ATDL)-1, Link-22, and Variable Message Format (VMF). In this capacity, DISA will:

a. Serve as DOD single point of contact for development and configuration management of joint TDL message standards. In accordance with reference e, DISA will execute the responsibilities of the lead standardization activity and preparing activity for TDL message standards.

b. In collaboration with other DOD components, identify information exchange requirements and develop standardized procedures and formats for information flow among NSS TDLs.

c. Maintain a list of approved TDL interface standards against which NSS must be certified.

d. Convene and chair the JMSWG. The JMSWG is the authority for development of US TDL message standards and the focal point for resolving standards issues related to US and combined TDL interoperability.

e. Convene and chair the JMTCCB. The JMTCCB approves all changes to US TDL message standards and associated documentation in accordance with reference c, and establishes US positions regarding allied or NATO TDL interoperability including all changes to STANAGs and associated documentation.

f. Identify, program, and provide resources to accomplish DISA responsibilities for TDL message standard management.

g. In accordance with DOD Regulation 5200.1-R (reference i) and paragraph (1) above, act as classification authority for TDL message standards.

7. DOD Responsibilities

a. The DOD CIO (responsibilities outlined in references j through l) will review Service compliance with TDL interoperability policies established by this instruction and references a through q (including reference m, the DOD Joint Technical Architecture). Based on this review and evaluation, the DOD CIO will make recommendations to the Defense Acquisition Executive (DAE) regarding program funding.

b. The DAE (reference n) will, either independently or based on recommendations from the DOD CIO and Military Department CIOs, take appropriate action to encourage program compliance with interoperability policy.

c. The DAE may direct the DOD Chief Financial Officer (reference o) and the heads of Military Departments to withhold acquisition program funds based on failure to comply with TDL interoperability policies, migration plans or interoperability shortfalls.

d. Office of the Assistant Secretary of Defense (Production and Logistics) Economic Security Division will manage and produce MIL-STDs and military bulletins (MIL-BULs) for the TDL program.

e. The Defense Printing Service is responsible for printing and distributing TDL CJCSMs, MIL-STDs, and MIL-BULs.

(INTENTIONALLY BLANK)

ENCLOSURE B

TDL STANDARDS PUBLICATIONS

<u>TDL</u>	<u>Associated Publications</u>
Link-11A/B	MIL-STD 6011
Link-4A	MIL-STD 6004
ATDL-1	MIL-STD 6013
Link-16	MIL-STD 6016
IBS CMF	IBS TIDP-TE
JRE	MIL-STD 3011
VMF	VMF TIDP-TE
Link-22	STANAG 5522 (no US MIL-STD equivalent)

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

- a. DOD Directive 4630.5, 11 January 2002, "Interoperability, and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- b. DOD Instruction 4630.8, 2 May 2002, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- c. Defense Information Systems Agency, Interoperability Directorate (IN5), Military C2 Standards Division, "Terms of Reference for the Joint Multi-TDL Configuration Control Board"
- d. Defense Information Systems Agency, Interoperability Directorate, Military Command and Control Standards Division, "Terms of Reference for the Joint Multi-TDL Standards Working Group"
- e. JIEO Plan 3200, November 1993, "Department of Defense Information Technology Standards Management Plan"
- f. CJCS Manual 6120.01C, Change 1, 1 June 2003, "Joint Multi-Tactical Data Link Operating Procedures"
- g. CJCS Instruction 6212.01 Series, 8 May 2000, "Interoperability and Supportability of National Security Systems and Information Technology Systems"
- h. Assistant Secretary of Defense for Command, Control, Communications and Intelligence, June 2000 "Joint Tactical Data Link Management Plan"
- i. DOD Regulation 5200.1-R, 7 June 1992, "Information Security Program Regulation"
- j. Title 10, US Code, Chapter 131, "Planning and Coordination"
- k. Title 44, US Code, Chapter 25, "Information Technology Management" and Chapter 35, "Coordination of Federal Information Policy"
- l. DOD Directive 5137.1, 12 February 1992, "Assistant Secretary of Defense for Command, Control, Communications and Intelligence"

- m. Department of Defense Joint Technical Architecture 3.0
 - o. DOD Directive 5134.1, 21 April 2000, “Under Secretary of Defense for Acquisition, Technology and Logistics”
 - p. DOD Directive 5118.3, 6 January 1997, “Under Secretary of Defense (Comptroller) (USD(C)), Chief Financial Officer (CFO), Department of Defense”
 - q. Global Information Grid Capstone Requirements Document (GIG CRD) JROCM 134-01, 30 August 2001

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

ATDL	Army tactical data link
C/S/A	combatant command/Service/Agency
C3I	command, control, communications and intelligence
CIO	Chief Information Officer
CMF	common message format
CRD	Capstone Requirements Document
DAE	Defense Acquisition Executive
DISA	Defense Information Systems Agency
DSP	Defense Standardization Program
IATO	interim authority to operate
IBS	integrated broadcast service
IER	information exchange requirement
IN	Interoperability Directorate
IOP	interface operating procedures
ITP	interoperability test panel
ISRP	interoperability senior review panel
ITS	information technology system
IWL	interoperability watch list
JINTACCS	joint interoperability of tactical command and control systems
JITC	joint interoperability test command
JMSWG	Joint Multi-Tactical Data Link Standards Working Group
JMTCCB	Joint Multi-Tactical Data Link Configuration Control Board
JTDLMP	Joint Tactical Data Link Management Plan
MCEB	Military Communications-Electronics Board
MIL-BUL	military bulletin
MIL-STD	military standard
NATO	North Atlantic Treaty Organization

NSS	National Security Systems
SIAP-SE TF	Single Integrated Air Picture-System Engineering Task Force
STANAG	Standardization Agreements
TDL	tactical data link
USJFCOM	US Joint Forces Command
VMF	variable message format

PART II--DEFINITIONS

configuration item (CI) -- An aggregation of hardware and software that satisfies and end use function and is designated by the government for separate configuration management. (JIEO Plan 3200 applies the term “CI” to Information Technology standards that are under configuration management).

configuration management -- As applied to configuration items, a discipline applying technical and administrative direction and surveillance over the life cycle of items. (Refer to JIEO Plan 3200 for further explanation). The Joint Multi-Tactical Data Link Configuration Control Board uses this management process to develop and maintain joint tactical data link standards, interface operating procedures and associated documents and to establish US positions regarding allied or NATO interoperability.

exception -- An exception is the permanent deviation of a system’s TDL implementation from the required TDL standard minimum implementation. Exceptions are approved by the JMTCCB. Systems granted an exception are subject to joint certification testing.

interim authority to operate (IATO) -- IATO represents the authority to field a new system or capability for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an IATO will be made by the Military Communications-Electronics Board Interoperability Policy and Test Panel based on the sponsoring component’s initial laboratory test results and assessed impact, if any, on the operational network to be employed.

information technology system (ITS) -- ITS includes any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

interface operating procedures (IOP) -- IOPs are published in CJCSM 6120.01 and provide doctrine, tactics, techniques and procedures designed for combatant commands, joint task force commanders,

Services and agencies in planning, designing and operating TDL networks.

Interoperability Directorate (IN), Military Command and Control Standards Division DISA -- functions as Lead Standardization Activity and Preparing Activity for TDL standards.

Joint Interoperability of Tactical Command and Control Systems (JINTACCS) -- The JINTACCS program is managed in accordance with this and other referenced instructions and includes TDLs and US Message Text Formats.

joint interoperability test command (JITC) -- DISA (JITC) is responsible for NSS interoperability certification.

Joint Multi-TDL Standards Working Group (JMSWG) -- The JMSWG is the joint body chaired by DISA tasked with resolving joint and combined interoperability issues affecting the JINTACCS TDL program.

Joint Multi-TDL Configuration Control Board (JMTCCB) -- The JMTCCB is a joint board chaired, funded and coordinated by DISA and is responsible for configuration management of the JINTACCS TDL message standards process.

National Security Systems (NSS) -- NSS include telecommunications and information systems operated by the Department of Defense, the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

TDL message standards -- TDL message standards are a set of technical and procedural parameters with which systems/equipment must comply to achieve compatibility and interoperability with other systems/equipment. This includes the data communications protocol and data item implementation specification.

tactical data link (TDL) -- A TDL is a standardized communications link suitable for transmission and receipt of tactical digital information. TDLs interface two or more command and control or weapons systems via

single network architecture and multiple communication media. Current practice is to characterize a TDL by its standardized message formats and transmission characteristics.

technical interface design plan test edition (TIDP-TE) -- Under the joint publication CM process, interim TDL standards are developed as TIDP-TEs to conduct developmental certification testing.

variable message format (VMF) -- VMF is a message format designed to support the exchange of digital data between combat units with diverse needs for volume and detail of information using various communications media. VMF is a bit-oriented message standard with limited character-oriented fields. Message length can vary with each use based on the information content of the message. VMF is intended to be the basis of the US Army's digitization transformation.

(INTENTIONALLY BLANK)